情报驱动的安全运营体系

基于腾讯云的安全运营实践





关于我 为什么做情报 情报驱动的

情报驱动的安全运营体系



关于我心体

oppo



关于云鼎实验室

腾讯安全云鼎实验室专注云安全技术研究 和云安全产品创新工作;负责腾讯云安全 架构设计、腾讯云安全防护和运营工作; 通过攻防对抗、合规审计搭建管控体系, 提升腾讯云整体安全能力。



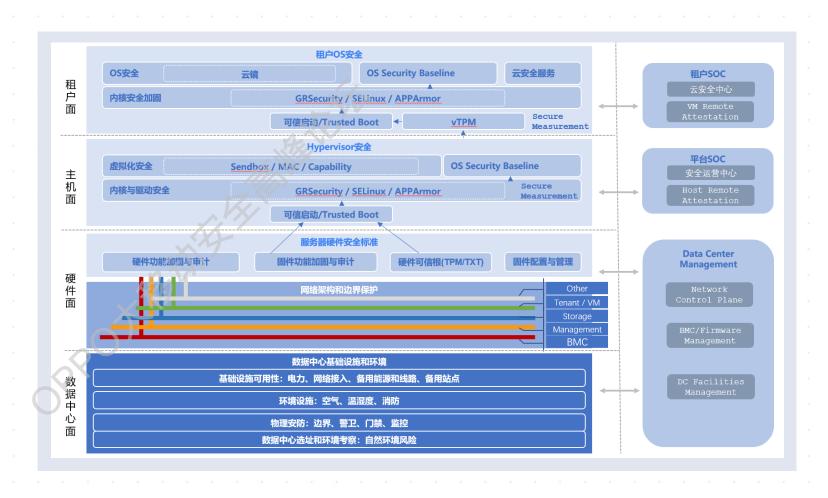


图 腾讯云全栈安全基础设施





为什么做情报

2017年"永恒之蓝"漏洞爆发,肆虐全球



- 5月12日,WannaCry蠕虫病毒在互联网上大肆爆发
- 影响到全球 近百个国家上千家企业 及公共组织
- 社交媒体微信、微博、科技媒体、安全媒体、博客等快速传播发酵





团队对"永恒之蓝"漏洞的复盘思考



重大漏洞来临, 云服务商需要做什么, 从哪里开始做, 如何评价做得好不好?

- ①如何更快发现,并提醒业务做好防范?
- ②修复时间 VS 系统稳定性 平衡?
- ③云环境下修复对象包含哪些?
- ④修复指标如何衡量?
- ⑤针对批量利用,如何快速止损?
- ⑥已中招用户如何引导修复?
- ⑦外部安全舆情危机及内部询问,如何应对?

•••••





"永恒之蓝"漏洞应急响应启示——时间窗口



时间×效率×指标

(漏洞发现) × (流程规范工具) × (审计手段)

(事前响应) × (事中处理) × (事后优化)

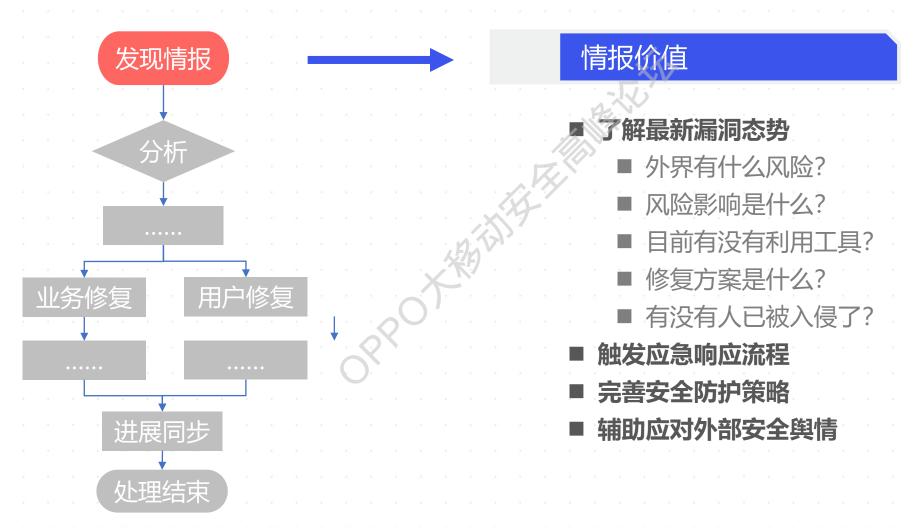
那么,如何跟黑客赛跑,争取更大的时间窗口?



情报是扩大时间窗口的核心武器



只有知道外部新出现哪些漏洞或威胁,才能第一时间启动应急响应,为业务预留更多修复时间窗口







03

情报驱动的安全运营实践

对安全情报的理解





漏洞情报

威胁 情报 事件 情报

属于内部情报,确定己方信息资产, 用于风险评估,如通过资产测绘等 方式发现 偏向于软硬件系统已 知未知漏洞,常用于 风险评估和漏洞管理

偏向于对攻击源的行 为画像分析,描述其 技术风格、惯用手法 偏向于对已经发生的安全事件 的媒体报道,有助于管理者对 类似风险进行参考借鉴

2

3

安全情报

Security Intelligence

4



如何获取最新的漏洞情报——了解漏洞的生命周期



漏洞出生



漏洞成长



漏洞爆发



漏洞死亡

- 关键标识:
 - CVE申请
 - 社区邮件列表
 - ・官方公告
 - ・安全博客

- 关键标识:
 - 开源社区
 - •漏洞细节
 - · 公开PoC

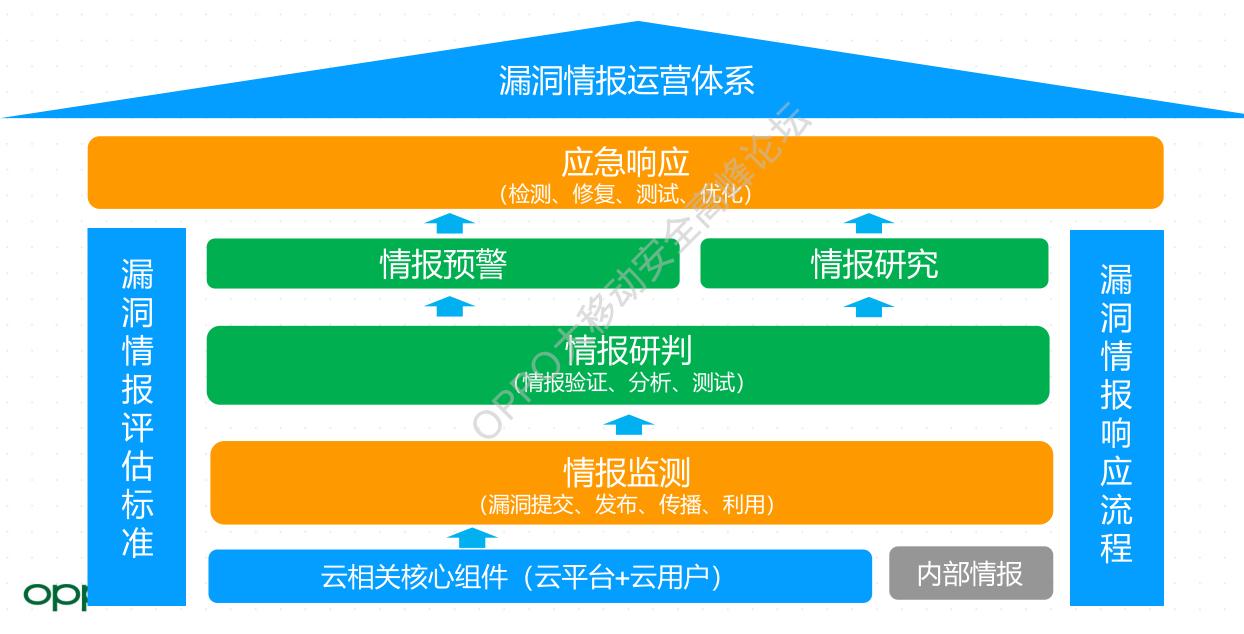
- 关键标识:
 - 自动化工具
 - 大规模传播
 - 媒体报道

- 关键标识:
 - ・技术分析
 - 淡出视野



漏洞情报体系设计思路

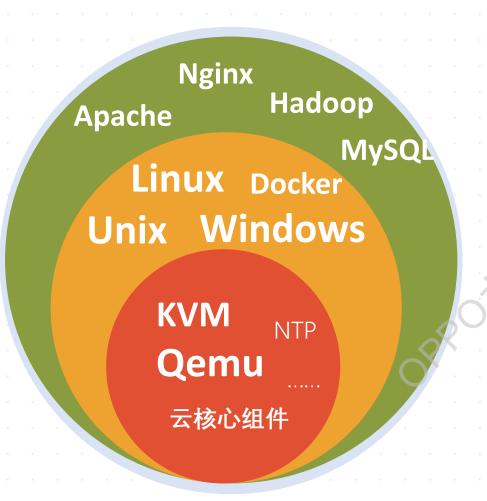




关于监控目标的选择——定位云相关核心组件



基于数百次重大漏洞应急总结,梳理出云相关核心系统或组件,建立核心资产漏洞监测列表 (110+)





情报监测:分析维护一手情报渠道,高频捕获



300+情报源, 21种渠道类型, 30分钟全渠道捕获

部

获

的

报

社交网络发布

漏洞作者或团队发布

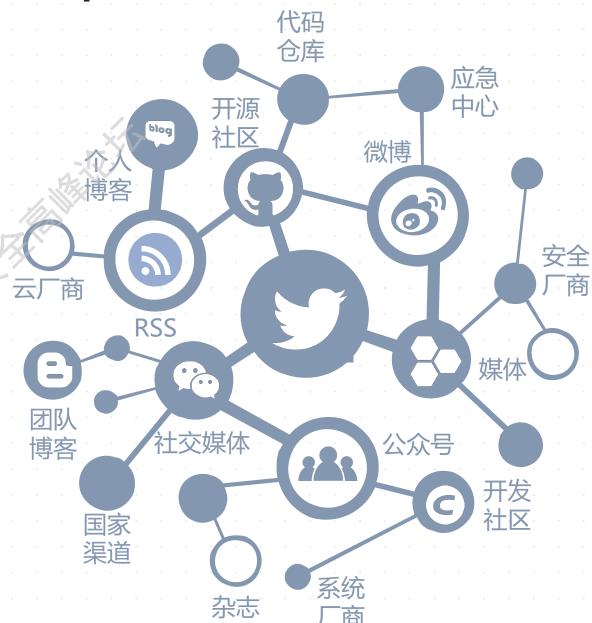
公众号发布

官方或组件厂商发布

安全厂商发布

新闻媒体发布

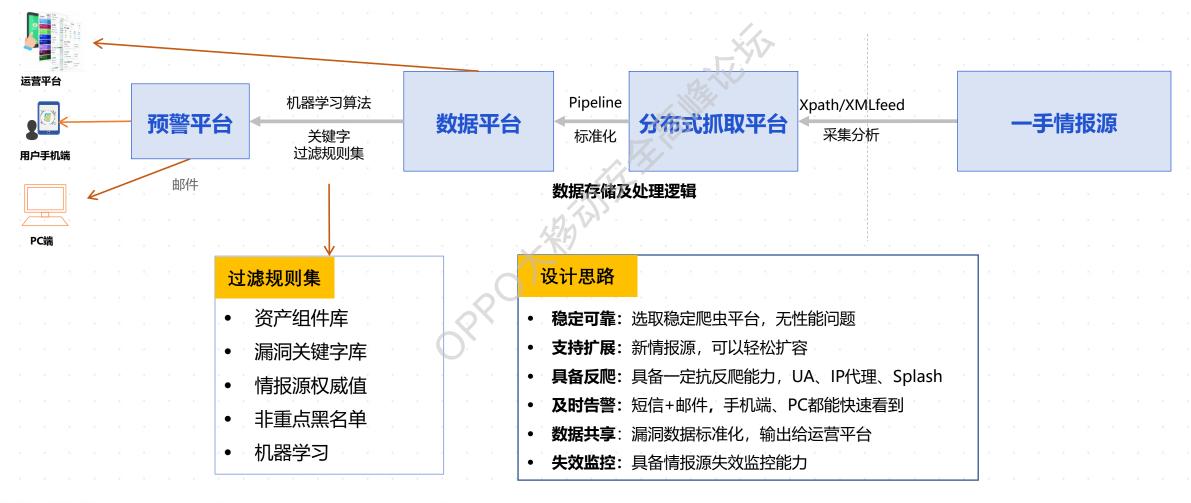
掌握历史漏洞作者或团队的漏 洞发布位置并进行捕获,是获 取一手情报源的关键





技术实现:基于开源爬虫框架设计,高扩展,稳定性强 eck

系统每周可以捕获到6000多个情报,经过自动化过滤,可以筛选出400左右的目标情报

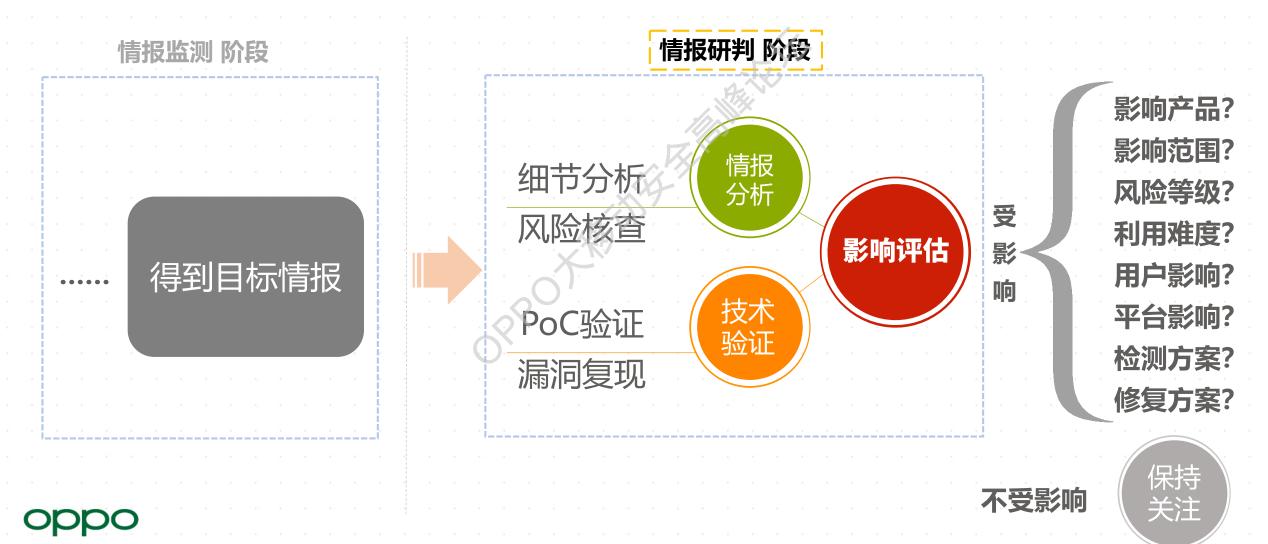




情报研判:整个情报运营体系中最重要的一步



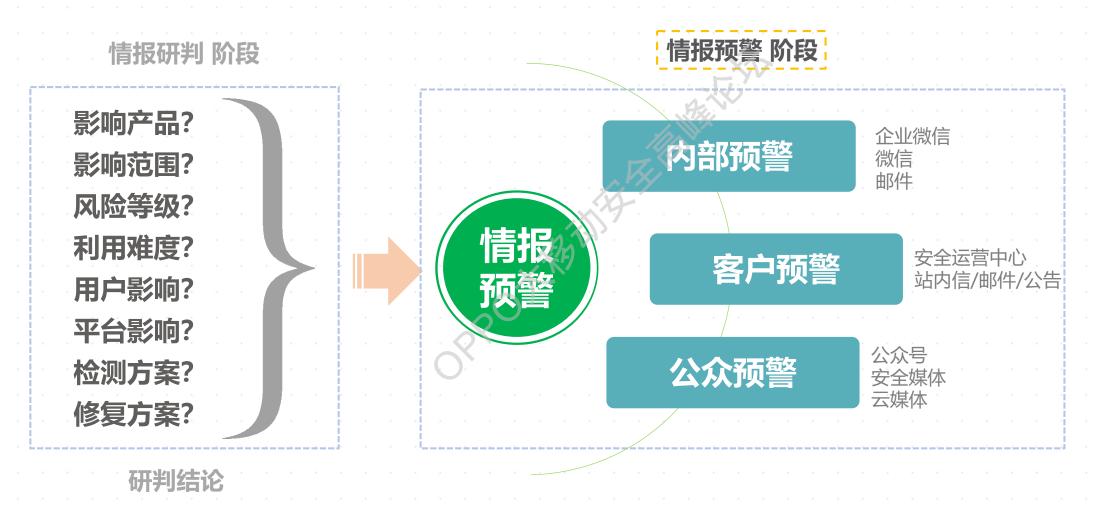
从原始情报提取出价值情报,除过滤规则库外,还需要人工介入进展**技术分析、验证测试**,确认情报程度及影响面



情报预警: 对内和对外提供多种预警方式



确认价值情报后,进入情报预警阶段,知会相关风险及修复建议给相应团队及用户,进入应急响应控制风险





情报研究: 针对基础设施或通用问题进行专题研究



结合情报对基础设施(固件、容器服务、虚拟化服务等)的影响范围和危害程度,进行专项深度研究

情报研判 阶段

影响产品?

影响范围?

风险等级?

利用难度?

用户影响?

平台影响?

检测方案?

修复方案?

影响 核心基础 设施 情报专题研究

基础固件

容器服务

虚拟化组件

•••••

以点带面, 系统研究

专题 研究

研判结论



应急响应: 为内外部事件处置提供运营决策支撑



应急响应 即情报的深度赋能阶段,通过监控漏洞利用、传播、事件态势,为内部响应修复提供运营决策指导



情报运营过程中的挑战与解决手段



情报运营重点解决两类问题:

- 1、系统误报漏报优化,针对漏报、误报情况,完善情报源并优化相关规则
- 2、持续监控利用,监控漏洞利用传播情况,调整修复策略

典型问题

漏报

误报

反爬

情报源失效

.....



情报运营 阶段

漏报解决

查漏补缺,新增情报源或规则完善

误报解决

调整策略, 优化情报监测规则

反爬措施

持续对抗,了解网站反爬规则

失效解决

反向验证,监控后开发新爬虫

... 运营

持续利用监控,变种舆情监控 ...



情报腾讯云安全运营中心对外输出



... (i) at | 4G at | 82

安全运营中心

₩ 安全概览

三 安全事件

☆ 漏洞管理

安全情报

→ 泄露监测

□ 安全大屏

② 服务管理

● 产品设置

参 腾讯云

【安全预警】Apache Hadoop权限提升漏洞风险预警

TCSA-2019-0026



可用性影响 (A)

机密性影响 (C)

文击难度 (AC)

权限要求 (PR)

完整性影响(1)

情报概览

风险等级 高危

CVSS 评分 8.8

CVE 编号 CVE-2018-8029

腾讯云安全中心监测到Apache Hadoop 被爆存在本地提权漏洞(C

VE-2018-8029) ,攻击者利用该漏洞可将能提升到 yarn 权限的帐

户提升到 root 最高权限。

为避免您的业务受影响, 腾讯云安全中心建议您及时开展安全自

查,如在受影响范围,请您及时进行更新修复,避免被外部攻击者

入侵

本地权限提升

2019-05-31 11:02:23

情报详情

Apache Hadoop 多个版本被爆存在本地提权漏洞(CVE-2018-8029),利用该漏洞,攻击者可将任意能提升到 yarn 权限的用户提升 到 root 权限,以执行恶意代码

Apache Hadoop 3.0.0-alpha1 到 3.1.0 版本 Apache Hadoop 2.9.0 到 2.9.1 版本 Apache Hadoop 2.2.0 到 2.8.4 版本

腾讯云安全运营中心



106919298820980

2 2-13 19:08

16:17

【腾讯云】尊敬的用户(账号ID:

100007805063, 昵称: 云安全-平台安

全),您好!腾讯云态势感知发布了最

新安全情报,请您关注:

情报名称: Nexus Repository

Manager 3 访问控制缺失及远程代码

执行漏洞预警 风险等级:严重

详情请点击: https://console.cloud

.tencent.com/sa/screen/info.html?id

=TCSA-2019-0019 •

短信





THANKS

